Guidelines for Implementing Secure Access to HPCMP Systems

1.0 Introduction

The High Performance Computing Modernization Program (HPCMP) provides DoD researchers access to one of the best collections of high performance computers available in the world. The program also provides high capacity, low latency networking, second to none, in the form of the Defense Research and Engineering Network (DREN). With this capability available, it is inevitable that new applications will be developed requiring that multiple, geographically dispersed hosts communicate across the wide area network.

These new applications may require access to HPCMP shared resources using mechanisms other than the HPCMP prescribed Kerberos/SecurID. This document defines processes for approving new access methods and provides guidelines that can be used in developing these mechanisms. This document is intentionally kept to a high level to avoid unnecessary restrictions on the developer. Use of these processes and guidelines allows development and use of these new access methods without compromising the integrity of the HPCMP security posture.

2.0 Scope

This document provides guidelines for approving new methods of accessing HPCMP shared computational resources at all HPCMP centers. Any access to HPCMP shared computational resources which are not covered by this document must be approved by the HPCMP designated approving authority (DAA).

3.0 Overview

For purposes of the document:

1. "access" is defined as a connection to a server. This specifically includes the following cases:
   a. Traditional client-server applications (telnet, ftp, ssh, etc.).
   b. Peer-to-peer applications in which the server also functions as a client.
   c. System-to-system applications where the client is a special purpose account rather than a regular user.
   This list is not comprehensive. Access to servers via a mechanism other than those listed above must still be approved in accordance with the guidelines in this document.
2. A "service" is defined as a functionality provided by the server, including but not limited to:
   a. Data transfer, predefined files
   b. Data transfer, arbitrary files
   c. Command execution, predefined commands
   d. Command execution, arbitrary commands (shell access)
3. "local approval" is defined as permission to implement a new access method to or service on HPCMP systems granted by on-site management personnel responsible for their operation and security.
4. "local approval authority (LAA)" is defined as an individual authorized to grant local approval. Generally, this is the local DAA or someone who has been delegated DAA authority at the site.
5. "HPCMP approval" is defined as permission to implement a new access method to or service on HPCMP systems granted by the HPCMP DAA.

4.0 Approval Process

Services included with an official operating system release are approved for use on HPCMP shared resources unless specifically prohibited. The HPCMO will maintain a database of other approved services that should be consulted by developers before beginning new efforts. Time and resources can be saved by reusing existing approved services.

All newly developed services or access methods that have not been previously approved by the HPCMP will require approval by the LAA before being implemented on an HPCMP system. If multiple HPCMP centers are involved, local approval is required at each individual center. To initiate the approval process, the following must be provided to the LAA by the developer:

1. A description of the proposed service including:
    a. The category of the service:
        i. Data transfer, predefined files
        ii. Data transfer, arbitrary files
        iii. Command execution, predefined commands
        iv. Command execution, arbitrary commands (shell access)
        v. Other (describe separately)
    b. The purpose of the service.
    c. A description of the data and/or commands to be accessed. It should be specified whether data access is read, write, or both.
    d. A description of the clients that will access the service. This can be provided as a list of individual hosts, a community of interest, or other appropriate grouping.
    e. The sensitivity of any data to be accessed.
    f. The level at which the service is to run (user versus privileged) and the level of access required (access to root or any other non-user accounts, indirect access via setuid, setgid, or other means).
    g. The platforms for which the service is being developed.
    h. The length of time the service must remain available.
2. A written protocol definition or Request for Comments reference.
3. A list of the HPCMP centers where the service will be implemented.
4. **An explanation of the authentication mechanism being implemented with this service.** Some type of authentication mechanism is required as called for in Paragraph 5.0.
5. A diagram of the client server architecture.
6. A diagram showing the data flow of the proposed service.
7. One of the following:
    a. a copy of the source code for the server and client or
    b. a warranty statement covering the affected code or
    c. approval from the local approval authority to proceed without a or b.
8. Any other information that will aid the reviewers in understanding the implementation of the service.
9. A statement that the list of approved services maintained by the HPCMP Office (HPCMPO) has been examined and that no previously approved service will provide the needed functionality.
10. A description of any special security features the service provides or incorporates.

Proprietary designs or designs requiring a non-disclosure agreement should not be submitted and will not be considered for approval.

A decision will be rendered by the LAA once the review is complete. This decision is final with the following exception: Services that provide execution of arbitrary commands that allow execution of privileged commands (executables owned by root with SUID set, for example), or that run at a privileged level must also be approved by the HPCMP before they are implemented on an HPCMP system.

Once local approval for a service is given, the original package plus a copy of the LAA's decision and any other documentation the LAA feels is appropriate will be provided to the HPCMP DAA. If HPCMP review is required, it will be completed within 60 days. In all cases, the HPCMP will add a description of the approved service to the approved services database with contact information to facilitate the reuse of approved services.

4.1 Changes After Approval

Once the new service or access method has been approved, the LAA must be notified of any changes to the items in section 4.0. The LAA will then determine if a new review is required. The LAA will then provide a copy of the changes to the HPCMP DAA. The HPCMP DAA may also require a new review if warranted.

4.2 Verification

Comprehensive security assessment (CSA) teams will be provided with approval packages and will verify that any services and access methods approved under these guidelines have been properly implemented and are being used appropriately

5.0 Approval criteria for service categories

Authentication and encryption for command execution and data transfer services should be commensurate with the sensitivity of the commands and/or data provided. Services which provide shell access or arbitrary command execution must provide user authentication, encryption, and host identification on par with the existing Kerberos/SecurID system. Services which could expose user logon credentials (such as keys or passwords), information protected under the Privacy Act of 1974 (5 U.S.C. § 552a), or other equally sensitive information must use strong encryption (3DES or AES) and provide host identification at least equal to that provided by Kerberos. Authentication for sensitive services should use hardware tokens if possible; otherwise (as in unattended system-to-system access) a public/private or shared key pair must be used. In cases where the commands and data are no more sensitive than in existing unauthenticated Unix services (DNS for example), the service may be provided without any encryption or authentication.

5.1 Data transfer, predefined files

This is the simplest category of service. Only data and files that are predefined and identified during the approval process can be accessed by clients. This information must be well defined and easily identifiable. The server must include a mechanism for explicitly identifying information that may be accessed and denying access to all other. This can be as simple as allowing only certain fully qualified filenames but the use of additional restrictions, such as a chroot “jail,” are recommended.

The level of authentication and encryption required for this category of service must be in accordance with section 5.0. Local approval at the center where access is to be provided is permitted for a service of this type.

5.2 Data transfer, arbitrary files

This category of service allows the reading and writing of arbitrary files to a user directory. The contents of these files can vary according to the application. These services can provide capabilities necessary to facilitate the transfer of arbitrary files that are not necessary with predefined files, such as viewing filenames, traversing directories, etc.

Approval of these services requires that the file space where reading and writing are authorized be well defined, and that a mechanism is in place to prevent access to other data, especially system files and data owned by other users.

The level of authentication and encryption required for this category of service must be in accordance with section 5.0. Local approval at the center where access is to be provided is permitted for a service of this type.

5.3 Command execution, predefined commands

These services support remote execution of a limited set of predefined commands. The predefined commands may be built-in (implemented by the new service itself) or the service may run a subset of the commands provided on the system by the system vendor or by third parties. Documentation for the service must include a detailed description of each command. For system provided commands, a description provided by the system, such as a Unix man page, will suffice. Documentation provided for built-in commands must include at least the level of detail found in Unix

man pages. In all cases the documentation must clearly note any commands which will be run setuid or setgid to another account.

The level of authentication and encryption required for this category of service must be in accordance with section 5.0. In general, services of this type may be approved locally. However, if any commands require setuid/setgid to root or another privileged account the service will be considered to require root access and will require HPCMP approval before implementation.

5.4 Command execution, arbitrary commands

Services of this type allow execution of commands not confined to a predefined set. Because of the risk inherent in this type of access, strong authentication as approved by the HPCMP is required. The service must also implement logging of all access and actions. Approval of the SRC Director is required, followed by approval of the HPCMP DAA.

6.0 Exceptions

At the request of the center director, the HPCMP DAA may approve the use of a service on HPCMP shared resources for a period of fourteen days even though the approval process is not completed as long as the required documentation has been provided. The reason for such an exception must be an unforeseen circumstance requiring acceleration of the mission schedule. The intention of this paragraph is not to compensate for a lack of preparation on the part of the developer.

7.0 Conclusion

This document attempts to define procedures and criteria that will cover most types of access to HPCMP resources which users are likely to develop in the future. However, it is almost certain that some form of access will become necessary that is not covered by this document. In such a case the developer should contact the HPCMPO for guidance.

This document is to be considered a living document. As it is applied to various situations, shortcomings and errors will be found. These should be addressed as soon as possible. In addition, this document should be reviewed on a regular basis by the Security Implementation Group and the Security Working Group to determine if any changes, additions, or deletions are necessary.